IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application:	:	Group Art Unit: 2136
James P. Goddard	:	Examiner: Daniel L. Hoang
Serial No.: 10/690,017	:	IBM Corporation
Filed: 10/21/2003	:	Intellectual Property Law
Confirmation No.: 4833	:	Department SHBC/040-3
Title: SYSTEM, METHOD AND PROGRAM	:	1701 North Street
PRODUCT TO DETERMINE SECURITY	:	Endicott, NY 13760
RISK OF AN APPLICATION	:	

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

I. REAL PARTY IN INTEREST

International Business Machines Corporation is the real party in interest.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

III. STATUS OF CLAIMS

Claims 1, 3, 7-10, 12, 15, 19-20 and 25-37 are pending, Finally Rejected and Appealed.

Claims 2, 4-6, 11, 13-14, 16-18 and 21-24 were previously canceled.

IV. STATUS OF AMENDMENTS

No amendment was submitted after Final Rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Support for each claim element is indicated in plain brackets [ ].

Claims 1 and 25 recite a computer implemented method and computer program product for evaluating a security risk of an application. [Computer program implementing automated processes 200 and 300.] A determination is made whether the application is shared by different customers [Decision 308 of Figure 3. Page 8 lines 16-17. First program instructions of original claim 24.] A determination is made whether a third party can have unauthorized administrative authority to data maintained by the application. [Decisions 212 and 225 of Figure 2. Page 7 lines 1-2 and 9-11.] A determination is made whether a third party can have unauthorized read and/or write access to data maintained by the application. [Decision 217 and 224 of Figure 2. Pages 7 lines 6-9.] A numerical value or weight is assigned to each of the foregoing determinations. [Steps 310, Step 226, Step 215, Step 222. Page 7 lines 6-15. Page 8 lines 17-18] Each of the numerical values or weights corresponds to a significance of the respective determination in evaluating the security risk. [Page 2 lines 7-10 and 16-18. Second program instructions of original claim 21] The numerical values or weights are combined to evaluate the security risk. [Page 4 lines 6-10. Page 7 lines 14-15, Step 310 and Page 8 lines 17-18, Steps 204, 215, 222 and 230, Page 7 lines 6-9 and 14-15].

Claim 32 recites a computer program product for evaluating a security risk of an application. [Computer program implementing automated processes 200 and 300.] First program instructions determine whether a vulnerability in the application can be exploited by a person or program which has not been authenticated to the application or a system in which the application runs. [Decision 240 of Figure 2. Page 7 lines 15-18.] Second program instructions determine whether a third party can have unauthorized administrative authority to data maintained by the application. [Decisions 212 and 225 of Figure 2. Page 7 lines 1-2 and 9-11.]

Third program instructions assign a numerical value or weight to each of the foregoing determinations. [Step 242 doubling a value assigned in step 214, 215, 222, 226 and/or 228. Page 7 lines 15-18. Step 226, Page 7 lines 9-11.] Each of the numerical values or weights correspond to a significance of the respective determination in evaluating the security risk. [Page 2 lines 7-10 and 17-18. Third determining step of original claim 22.] Fourth program instructions combine the numerical values or weights to evaluate the security risk. [Page 4 lines 6-10. Page 7 lines 14-15, Steps 240, 242 and 204, Steps 225, 226 and 230, Page 7 lines 6-9 and 14-15].

VI. Grounds of Rejection

Claim 12 was rejected under 35 USC 112, second paragraph because of the recitation "determining whether there is an intrusion detection system and vulnerability scanning for said application" in lines 3-4.

Claims 1, 7-10, 14, 25-29 and 32-34 were rejected under 35 USC 102(e) based on Goldfeder et al. (US Publication No. 20040230835).

Claims 3, 15, 19-20, 29, 30-31 and 35-37 were rejected under 35 USC 103(a) based on Goldfeder et al.

VII. Argument

A claim cannot be obvious under 35 USC 103 unless (a) there is a reason that a person of ordinary skill in the art would have combined the references, and (b) all the claim elements are taught or suggested by the prior art. See In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438, 1443 (Fed Cir. 1991) and KSR Int'l Co. v. Teleflex, Inc., No. 04-1350 (USSC 30 April 2007).

35 USC 112, second paragraph rejection of claim 12

Claim 12 was rejected under 35 USC 112, second paragraph because of the recitation "determining whether there is an intrusion detection system and vulnerability scanning for said application" in lines 3-4. The Examiner asserted that it was unclear "whether an intrusion detection system and vulnerability scanning exists in said application or whether intrusion detection systems and vulnerability scanning are performed on the application." Claim 12 recites the step of "determining whether there is an intrusion detection system and vulnerability scanning **for** said application". (Emphasis added) This is clear. The intrusion detection system and vulnerability scanning functions can be anywhere, as long as they perform the intrusion detection and vulnerability scanning **for** the application.

35 USC 102(e) Rejection of Claims 1, 7-10 and 14 based on Goldfeder et al.

Claim 1 recites a computer implemented method for evaluating a security risk of an application. A determination is made whether the application is shared by different customers. A determination is made whether a third party can have unauthorized administrative authority to data maintained by the application. A determination is made whether a third party can have unauthorized read and/or write access to data maintained by the application. A numerical value or weight is assigned to each of the foregoing determinations. Each of the numerical values or weights corresponds to a significance of the respective determination in evaluating the security risk. The numerical values or weights are combined to evaluate the security risk.

Goldfeder et al. recite "Most users understand that new programs can introduce viruses or other malicious code on their computers." Goldfeder et al. Paragraph 002 of the Background section. "The application 201 may contain a virus or it may constitute spy ware." Goldfeder et al. Paragraph 0018. Goldfeder et al. also disclose evaluation of a security risk of an application. "For instance a virus evaluator may be configured to examine each component of an application for the possibility that the application contains a virus." Goldfeder et al. Paragraph 0035. This is simply scanning the application itself for the presence of virus code. In contrast, the present invention as recited in claim 1 determines if an application is shared by different customers or vulnerable to some type of attack by external factors - a vulnerability where a third party can have unauthorized administrative authority to data maintained by said application or a third party can have unauthorized read and/or write access to data maintained by the application. The vulnerabilities recited in claim 1 are to external attacks not based on the presence of a virus in the application in contrast to Goldfeder et al. As noted in the Background section of the present patent application, "vulnerabilities can be caused by programming errors, configuration problems or application design errors."

Goldfeder et al. also disclose: "For instance, a scoring engine may have determined that the application has requested sufficient permissions to read and modify files on the computer, and to transmit data over a network connection. Based on that information, together with perhaps other evidence, a privacy evaluator may have determined that the application is likely to

share the user's information over the network." Goldfeder et al. Paragraph 0039. This is an analysis of an application to determine whether a virus has caused the application itself to be malicious, i.e. likely to have accessed files and improperly transmitted file data over a network. Goldfeder et al. do not disclose or even suggest the step of determining if an application itself is shared (used) by different customers as recited in claim 1. Moreover, Goldfeder et al. do not disclose or even suggest the step of determining whether a third party can have unauthorized **administrative authority** to data maintained by the application as recited in claim 1. Moreover, Goldfeder et al. do not disclose either of these determinations in a computer implemented process for evaluating a security risk. Therefore, the rejection of claim 1 under 35 USC 102 should be reversed (and no rejection under 35 USC 103 would be proper).

Claims 7-10 and 14 depend on claim 1 and therefore distinguish over Goldfeder et al. for the same reasons that claim 1 distinguishes thereover. Therefore, the rejection of claims 7-10 and 14 under 35 USC 102 should be reversed.

35 USC 102(e) Rejection of Claims 25-29
based on Goldfeder et al.

Independent claim 25 distinguishes over Goldfeder et al. for the same reasons that claim 1 distinguishes thereover. Therefore, the rejection of claim 25 under 35 USC 102 should be reversed (and no rejection under 35 USC 103 would be proper). Claims 26-29 depend on claim 25. There was no 35 USC 103 rejection of claim 25. Therefore, the rejection of claims 26-29 should be reversed.

35 USC 102(e) Rejection of Claims 32-34
based on Goldfeder et al.

Claim 32 recites a computer program product for evaluating a security risk of an application. First program instructions determine whether a vulnerability in the application can be exploited by a person or program which has not been authenticated to the application or a system in which the application runs. Second program instructions determine whether a third party can have unauthorized **administrative authority** to data maintained by the application.

Third program instructions assign a numerical value or weight to each of the foregoing determinations. Each of the numerical values or weights corresponds to a significance of the respective determination in evaluating the security risk. Fourth program instructions combine the numerical values or weights to evaluate the security risk.

As noted above, Goldfeder et al. recite "Most users understand that new programs can introduce viruses or other malicious code on their computers." Goldfeder et al. Paragraph 002 of the Background section. "The application 201 may contain a virus or it may constitute spy ware." Goldfeder et al. Paragraph 0018. Goldfeder et al. also recite "Most users understand that new programs can introduce viruses or other malicious code on their computers." Goldfeder et al. Paragraph 002 of the Background section. "The application 201 may contain a virus or it may constitute spy ware." Goldfeder et al. Paragraph 0018. Goldfeder et al. also disclose evaluation of a security risk of an application. "For instance a virus evaluator may be configured to examine each component of an application for the possibility that the application contains a virus." Goldfeder et al. Paragraph 0035. This is simply scanning the application itself for the presence of virus code. In contrast, the present invention as recited in claim 32 determines whether a **third party** can have unauthorized **administrative authority** to data maintained by the application. This is an external attack not based on the presence of a virus in the application in contrast to Goldfeder et al. As noted in the Background section of the present patent application, "vulnerabilities can be caused by programming errors, configuration problems or application design errors." Goldfeder et al. do not disclose or even suggest an assessment of security based on whether there is unauthorized **administrative authority**.

Goldfeder et al. also disclose: "For instance, a scoring engine may have determined that the application has requested sufficient permissions to read and modify files on the computer, and to transmit data over a network connection. Based on that information, together with perhaps other evidence, a privacy evaluator may have determined that the application is likely to share the user's information over the network." Goldfeder et al. Paragraph 0039. This is an analysis of an application to determine whether a virus in the application has caused the application to be malicious, i.e. likely to have accessed files and improperly transmitted file data over a network. In contrast, the present invention as recited in claim 32 determines if a **third**

party can have unauthorized **administrative authority** to data maintained by the application. This is a much different test than in Goldfeder et al. Goldfeder et al. do not disclose or even suggest this program step of claim 32. Moreover, Goldfeder et al. do not disclose this determination in a computer implemented process for evaluating a security risk. Therefore, the rejection of claim 32 under 35 USC 102 should be reversed (and no rejection under 35 USC 103 would be proper).

Claims 33-34 depend on claim 32 and therefore distinguish over Goldfeder et al. for the same reasons that claim 32 distinguishes thereover. There was no rejection of claim 32 under 35 USC 103. Therefore, the rejection of claims 33-34 should be reversed.

35 USC 103(a) rejection of Claims 3 and 19-20
Based on Goldfeder et al.

Claims 3 and 19-20 depend on claim 1. There was no 35 USC 103 rejection of claim 1. Claims 3 and 19-20 distinguish over Goldfeder et al. for the same reason that claim 1 distinguishes thereover. Therefore, the rejection of claims 3 and 19-20 under 35 USC 103 should also be reversed.

35 USC 103(a) rejection of Claims 15, 29 and 35
Based on Goldfeder et al.

Claim 15 depends on claim 1 and recites a computer implemented method as follows. A determination is made whether there is a requirement for authentication of the application or a system in which the application runs to other systems **before connection of the application or the system in which the application runs to said other systems**. A numerical value or weight is assigned to this determination and used in evaluating the security risk. To support the rejection, the Examiner merely makes a general assertion that "privacy concerns could obviously be addressed by requiring the application to authenticate itself." Goldfeder et al. do not disclose or even suggest the test of claim 15 in determining a security risk. Dependent claims 29 and 35 similarly distinguish over Goldfeder et al. Therefore, the rejection of claims 15, 29 and 35 under 35 USC 103 should be reversed.

35 USC 103(a) rejection of Claims 19-20, 30-31 and 36-37
Based on Goldfeder et al.

Claims 19-20, 30-31 and 36-37 depend on claims 1, 25 and 32, respectively. Therefore, claims 19-20, 30-31 and 36-37 distinguish over Goldfeder et al. for the same reasons that claims 1, 25 and 32, respectively, distinguish over Goldfeder et al.

Based on the foregoing, the rejection of the pending claims should be reversed.

Respectfully submitted,

Dated: 07/10/07
Telephone: 607-429-4368
Fax No.: 607-429-4119

/Arthur J. Samodovitz/
Arthur J. Samodovitz
Reg. No. 31,297

VIII. CLAIMS APPENDIX:

1. A computer implemented method for evaluating a security risk of an application, said method comprising the steps of:

determining whether the application is shared by different customers;

determining whether a third party can have unauthorized administrative authority to data maintained by said application;

determining whether a third party can have unauthorized read and/or write access to data maintained by said application;

assigning a numerical value or weight to each of the foregoing determinations, each of said numerical values or weights corresponding to a significance of the respective determination in evaluating said security risk; and

combining said numerical values or weights to evaluate said security risk.

3. A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether said application is subject to industry controls for security; and

assigning a numerical value or weight to the determination whether said application is subject to industry controls for security, and using the numerical value or weight for the determination whether said application is subject to industry controls for security in evaluating said security risk.

7. A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether a third party can have unauthorized read and write access to said data; and

assigning a numerical value or weight to the determination whether a third party can have unauthorized read and write access to said data, and using the numerical value or weight for the determination whether a third party can have unauthorized read and write access to said data in evaluating said security risk.

8. A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether a vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs; and

assigning a numerical value or weight to the determination whether the vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs and using the numerical value or weight to the determination whether the vulnerability in said application can be exploited by a program or person which has not been authenticated to said application or a system in which said application runs in evaluating said security risk.

9. A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether said data maintained by by said application is confidential; and wherein

the numerical value or weight assigned to the determination whether a third party can have unauthorized write access to said data is based in part on whether said data is confidential.

10. A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether a customer has direct use of said application; and

assigning a numerical value or weight to the determination whether a customer has direct use of said application, and using the numerical value or weight for the determination whether a customer has direct use of said application in evaluating said security risk.

12. A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether there is an intrusion detection system and vulnerability scanning for said application; and

assigning a numerical value or weight to the determination whether there is an intrusion detection system and vulnerability scanning for said application, and using the numerical value or weight for the determination whether there is an intrusion detection system and vulnerability scanning for said application in evaluating said security risk.

15. A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether there is a requirement for authentication of said application or a system in which said application runs to other systems before connection of said application or said system in which said application runs to said other systems; and

assigning a numerical value or weight to the determination whether there is a requirement for authentication of said application or a system in which said application runs to other systems before connection of said application or said system in which said application runs to said other systems, and using the numerical value or weight for said requirement for authentication in evaluating said security risk.

19. A computer implemented method as set forth in claim 1 further comprising the step of comparing the evaluation of said security risk to a cost savings provided by said application, and determining whether to certify said application for use based in part on said comparison.

20. A computer implemented method as set forth in claim 1 further comprising the step of comparing the evaluation of said security risk to a revenue provided by said application, and determining whether to certify said application for use based in part on said comparison.

25. A computer program product for evaluating a security risk of an application, said computer program product comprising:

a computer readable media;

first program instructions to determine whether the application is shared by different customers;

second program instructions to determine whether a third party can have unauthorized administrative authority to data maintained by said application;

third program instructions to determine whether a third party can have unauthorized read and/or write access to data maintained by said application;

fourth program instructions to assign a numerical value or weight to each of the foregoing determinations, each of said numerical values or weights corresponding to a significance of the respective determination in evaluating said security risk; and

fifth program instructions to combine said numerical values or weights to evaluate said security risk; and wherein

said first, second, third, fourth and fifth program instructions are recorded on said media.

26. A computer program product as set forth in claim 25 wherein:

said third program instructions determine whether a third party can have unauthorized read and write access to said data;

said fourth program instructions assign a numerical value or weight to the determination whether a third party can have unauthorized read and write access to said data; and

said fifth program instructions also use the numerical value or weight for the determination whether a third party can have unauthorized read and write access to said data in evaluating said security risk.

27. A computer program product as set forth in claim 25 further comprising:

sixth program instructions to determine whether a vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs; and

seventh program instructions to assign a numerical value or weight to the determination whether the vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs; and wherein

said fifth program instructions also use the numerical value or weight to the determination whether the vulnerability in said application can be exploited by a program or person which has not been authenticated to said application or a system in which said application runs to evaluate said security risk; and

said sixth and seventh program instructions are recorded on said media in functional form.

28. A computer program product as set forth in claim 25 further comprising:

sixth program instructions to determine whether a customer has direct use of said application; and

seventh program instructions to assign a numerical value or weight to the determination whether a customer has direct use of said application; and wherein

said fifth program instructions also use the numerical value or weight for the determination whether a customer has direct use of said application in evaluating said security risk; and

said sixth and seventh program instructions are recorded on said media.

29. A computer program product as set forth in claim 25 further comprising:

sixth program instructions to determine whether there is a requirement for authentication of said application or a system in which said application runs to other systems before connection of said application or said system in which said application runs to said other systems; and

fifth program instructions to assign a numerical value or weight to the determination whether there is said requirement for authentication; and wherein

said fifth program instructions also use the numerical value or weight for said requirement for authentication in evaluating said security risk; and

said sixth and seventh program instructions are recorded on said media.

30. A computer program product as set forth in claim 25 further comprising:

sixth program instructions to compare the evaluation of said security risk to a cost savings provided by said application, and determine whether to certify said application for use based in part on said comparison; and wherein

said sixth program instructions are recorded on said media.

31. A computer program product as set forth in claim 25 further comprising:

sixth program instructions to compare the evaluation of said security risk to a revenue provided by said application, and determine whether to certify said application for use based in part on said comparison; and wherein

said sixth program instructions are recorded on said media.

32. A computer program product for evaluating a security risk of an application, said computer program product comprising:

a computer readable media;

first program instructions to determine whether a vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs;

second program instructions to determine whether a third party can have unauthorized administrative authority to data maintained by said application;

third program instructions to assign a numerical value or weight to each of the foregoing determinations, each of said numerical values or weights corresponding to a significance of the respective determination in evaluating said security risk; and

fourth program instructions to combine said numerical values or weights to evaluate said security risk; and wherein

said first, second, third and fourth program instructions are recorded on said media.

33. A computer program product as set forth in claim 32 further comprising:

fifth program instructions to determine whether a third party can have unauthorized read and/or write access to data maintained by said application; and

sixth program instructions to assign a numerical value or weight to the determination whether a third party can have unauthorized read and/or write access to data maintained by said application; and wherein

said fourth program instructions also use the numerical value or weight to the determination whether a third party can have unauthorized read and/or write access to data maintained by said application to evaluate said security risk; and

said fifth and sixth program instructions are recorded on said media in functional form.

34. A computer program product as set forth in claim 32 further comprising:

fifth program instructions to determine whether a customer has direct use of said application; and

sixth program instructions to assign a numerical value or weight to the determination whether a customer has direct use of said application; and wherein

said fourth program instructions also use the numerical value or weight for the determination whether a customer has direct use of said application in evaluating said security risk; and

said fifth and sixth program instructions are recorded on said media.

35. A computer program product as set forth in claim 32 further comprising:

fifth program instructions to determine whether there is a requirement for authentication of said application or a system in which said application runs to other systems before connection of said application or said system in which said application runs to said other systems; and

sixth program instructions to assign a numerical value or weight to the determination whether there is said requirement for authentication of said application or said system; and wherein

said fourth program instructions also use the numerical value or weight for said requirement for authentication of said application or said system in evaluating said security risk; and

said fifth and sixth program instructions are recorded on said media.

36. A computer program product as set forth in claim 32 further comprising:

fifth program instructions to compare the evaluation of said security risk to a cost savings provided by said application, and determine whether to certify said application for use based in part on said comparison; and wherein

said fifth program instructions are recorded on said media.

37. A computer program product as set forth in claim 32 further comprising:

fifth program instructions to compare the evaluation of said security risk to a revenue provided by said application, and determine whether to certify said application for use based in part on said comparison; and wherein

said fifth program instructions are recorded on said media.

IX. Evidence Appendix

There is no evidence entered or relied upon in the appeal.

X. Related Proceedings Appendix

There are no related proceedings and therefore no copies of decisions to provide.